WEB SITE ADMINISTRATION

Table A1.1. Checklist

MISSION STATEMENT: Establishes policies, assigns responsibilities, and defines procedures for operating and maintaining unclassified Web sites and services. ***Note:*** All references are from DoD Web Site Administration Policies and Procedures, 25 Nov 98.			
1.1. CRITICAL:	**YES**	**NO**	**N/A**
1.1.1. Have web page owners/masters/administrators ensured the following information IS NOT contained on organizational web pages:			
1.1.1.1. For Official Use Only (FOUO) information?			
1.1.1.2. Military Operations & Exercises information about:			
1.1.1.2.1. Unit Organizations?			
1.1.1.2.2. Unit readiness specifically?			
1.1.1.2.3. Detailed mission statement?			
1.1.1.2.4. Specific Unit phone/fax numbers (secure and unsecured)?			
1.1.1.2.5. Time-Phase Force Deployment Data (TPFDD)?			
1.1.1.2.6. Ops schedules?			
1.1.1.2.7. Logistics support requirements:			
1.1.1.2.7.1. Medical?			
1.1.1.2.7.2. Civil Engineering?			
1.1.1.2.7.3. POL?			
1.1.1.2.7.4. Host nation support?			
1.1.1.2.7.5. Transportation?			
1.1.1.2.7.6 Munitions?			
1.1.1.2.8. Force Apportionment?			
1.1.1.2.9. Force Allocation?			
1.1.1.2.10. Unit Beddown information?			
1.1.1.2.11. Planning Guidance?			
1.1.1.2.12. Unit augmentation?			
1.1.1.2.13. Force Synchronization:			
1.1.1.2.13.1. Unit shortfalls			
1.1.1.2.14. Counter-terrorism information?			
1.1.1.2.15. Detailed Budget Reports?			
1.1.1.2.16. Images of Command and Control (C2) nodes?			
1.1.1.2.17. Inventory reports?			
1.1.1.2.18. Intelligence, Surveillance and Reconnaissance (ISR) Capabilities?			
1.1.1.2.19. Command, Control, Communications, Computers and Intelligence(C41) Architecture?			
	YES	**NO**	**N/A**

1.1.1.2.20. Non-Combatant Evacuation Operations (NEO) Plans or Ops?			
1.1.1.2.21. Counter-drug Ops?			
1.1.1.2.22. Unit Recall Rosters?			
1.1.1.2.23. Weapons Movements?			
1.1.1.2.24. Mobilization information?			
1.1.1.2.25. Detailed maps or installation photography?			
1.1.1.2.26. Standard Operating Procedures?			
1.1.1.2.27. Tactics, Techniques, and Procedures?			
1.1.1.2.28. Critical maintenance?			
1.2.1. Personnel information relating to:			
1.2.1.1. Social Security Account Numbers?			
1.2.1.2. Dates of birth?			
1.2.1.3 Home addresses?			
1.2.1.4. Telephone numbers other than duty office numbers? (**Note:** duty phone numbers of units described in C.3.2.1.6.2.2. of DoD 5400.7-R (reference (j) may not be posted.)			
1.2.1.5. Names, locations, and any other identifying information about family members of DoD employees and military personnel?			
1.2.1.6. Official travel itineraries of individuals and units before it is performed?			
1.2.1.7. Duty rosters, or detailed organizational charts and directories with names (as opposed to organizational charts, directories, general telephone numbers for commonly requested resources, services and contacts without names)?			
1.2.1.8. Internal DoD personnel rules and practices unless cleared for release to the public?			
1.2.1.9. Financial Disclosure Reports of Special Government Employees? (Ref: 5 USC App. 4, para 207 (a) (1) 2)			
4.2.1.1. Representation Rights and Duties, Labor Unions? (Ref: 5 USC, para 7114 (b) (4))			
1.2.1.11. Action on reports of Selection Boards? (Ref: 10 USC, para 618)			
1.2.1.12. Confidential Medical Records? (Ref: 10 USC, para 1102)			
1.2.1.13 Civil Service Examination? (Ref: 18 USC, para 1917)			
1.2.1.14. Drug Abuse Prevention/Rehabilitation Records? (Ref: 21 USC, para 1175)?			
1.2.1.15. Confidential of Patient Records? (Ref: 42 USC, para 290dd-2)			
1.2.1.16. Information Concerning US Personnel Classified as POW/MIA During Vietnam Conflict? (Ref: 42 USC, para 401)			
1.2.1.17. Information Identifying Employees of DIA, NRO, and NIMA? (Ref: 10 USC, para 424)			
	YES	**NO**	**N/A**

1.3.1. Proprietary Information submitted by a contractor and protected by a Limited Rights Statement or other agreement, and trade secrets, commercial and financial information submitted by an entity outside the government that considers the information to be protected from release to the public. Other specific provisions include			
1.3.1.1. Contractor Proposals? (Ref: 10 USC para 2305)			
1.3.1.2 Commercial or financial information received in confidence with loans, bids, contracts or proposals?			
1.3.1.3. Information received in confidence e.g. trade secrets, inventions, discoveries or other proprietary data?			
1.3.1.4. Statistical date and commercial or financial information concerning contract performance, income, profits, losses and expenditures, if offered and received in confidence from a contractor or potential contractor?			
1.3.1.5. Scientific and manufacturing processes or developments concerning technical or scientific data and other information submitted with an application for research grant or with a report while research is in progress?			
1.3.1.6. Test and evaluation of commercial products or military hardware produced by a non-government entity?			
1.3.1.7. Patents, unless licensed for publication by the United States?			
1.3.1.8. Software documentation: shall be distributed according to the terms of the software license?			
1.3.1.9. Premature Dissemination: The information related to patentable military systems or processes in the development stage:			
1.3.1.9.1. Confidential Status of Patent Applications? (Ref: 35 USC para 122)			
1.3.1.9.2. Secrecy of Certain Inventions and Withholding of Patents? (Ref: 35 USC paras 181-188)			
1.3.1.9.3. Confidential Inventions Information? (Ref: 35 USC para 205)			
1.4.1. Test and Evaluation information that could result in an unfair advantage or disadvantage to the manufacturer or producer or could reveal the capabilities, limitations, or incapabilities of a DoD weapons systems or component?			
1.5.1. Scientific and technological information relating to:			
1.5.1.1. Critical technology on either the Munitions List or the Commerce Control List?			
1.5.1.2. Unclassified Special Nuclear Weapons Information? (Ref: 10 USC para 128)			
	YES	**NO**	**N/A**
1.5.1.3. Unclassified Technical Data with Military or Space			

Application? (Ref: 10 USC, para 130)			
1.5.1.4. Centers for Industrial Technology – Reports of Technology Innovations? (Ref: 15 USC, para 3705 (e)(E))			
1.5.1.5. Information Regarding Atomic Energy? (Ref: 42 USC, paras 2161-2168)			
1.5.1.6. Control of Arms Exports See 38(e) of the Arms Export Control Act? (Ref: 22 USC, para 2778(e))			
1.5.1.7. Technical and scientific data developed by a contractor or subcontractor exclusively or in part at private expense?			
1.5.1.8. Sensitive S & T reports such as:			
1.5.1.8.1. Defense Acquisition Executive System Reports?			
1.5.1.8.2. Selected Acquisition Reports?			
1.5.1.8.3. Weapons System Unit Cost Reports?			
1.5.1.8.4. Approved Program Baselines for ACAT I, II, III Weapons Systems?			
1.5.1.8.5. Weapons Systems Evaluation and Testing Results and Reports?			
1.5.1.8.6. Reports Based on Joint USA and Foreign Government Technical Research and Weapons Systems Evaluations?			
1.5.1.8.7. Weapons System Contractor Performance Reporting Under earned Value Reporting System at the Level of CPE Reporting?			
1.5.1.8.8. Weapons Systems staff working papers, correspondence and staff assessments?			
1.5.1.8.9. DoD Component “Feedback” staff working papers and assessments on weapons System Program Performance?			
1.6.1. Intelligence information relating to:			
1.6.1.1. Organizational & Personnel Information for DIA, NRO and NIMA? (Ref: 10 USC, para 424)			
1.6.1.2. Maps, Charts, and Geodetic Date? (Ref: 10 USC, para 455)			
1.6.1.3. Communications Intelligence? (Ref: 18 USC, para 798)			
1.6.1.4. NSA Functions and Information? (Ref: 50 USC, para 402)			
1.6.1.5. Protection of Identities of US Undercover Intelligence Officers, Agents, Informants and Sources? (Ref: 50 USC, para 421)			
1.6.1.6. Protection of Intelligence Sources and Methods? (Ref: 50 USC, para 403(d)(3))			
4.2.1. Other information relating to:			
1.7.1.1. A-76 studies and other outsourcing studies that provide detailed descriptions of sensitive organizational operations?			
	YES	**NO**	**N/A**
1.7.1.2. Administrative Dispute Resolutions? (Ref: 5 USC, para			

574(j))			
1.7.1.3. Confidentiality of Financial records? (Ref: 12 USC, para 3403)			
1.7.1.4. National Historic Preservation? (Ref: 16 USC, para 470w-3)			
1.7.1.5. Internal advice, recommendations and subjective evaluations?			
1.8.1. Security and Access Controls relating to:			
1.8.1.1. Sensitivity of information and target audience? (Use Part V, Examples & Best Practices, Table 1 to determine vulnerability of various combinations of information.)			
1.9.1. Privacy and Security Notices:			
1.9.1.1. Have Privacy and Security Notices been used?			
1.9.1.1.1. If Privacy and Security Notices have been used, have they been approved by the appropriate local legal authority before use?			
1.9.1.2. Have privacy and security notices been tailored?			
1.9.1.2.1. If privacy and security notices have been tailored, do they follow the guidance prescribed in Part V, Examples & Best Practices, Para 4, Text of Privacy and Security Notices?			

If access control is:	and transmission control is:	the vulnerability is:	and the information posted can be:
Open – Includes Webmaster training and certification, isolation of the server, current version of server software and O/S, with all security patches properly installed	Plain text, unencrypted	Extremely High -- Subject to worldwide dissemination and access by everyone on Internet	Non-sensitive, of general interest to the public, cleared and authorized for public release for which worldwide dissemination poses limited risk for DoD or DoD personnel, even if aggregated with other information reasonably expected to be in public domain.
Limited by Internet Domain (e.g. .mil, .gov) or IP address	Plain text, unencrypted	Very High -- Can circumvent access controls, affords lowest level of access control, and no encryption	Non-sensitive, not of general interest to the public although approved and authorized for public release, and intended for DoD or other specifically targeted audience.
Limited By User ID and password (e.g. DMDC database or other registration system)	Plain text, unencrypted	High -- Can circumvent access controls, affords higher level of access controls, however, IDs and passwords can be compromised if encryption is not used.	Non-sensitive but limited to a specific, targeted audience.
User Certificate Based (Software) Requires PKI	Encrypted text through use of secure sockets layer	Moderate -- Provides moderate level of access controls	FOR OFFICIAL USE ONLY and information sensitive by aggregation
User Certificate Based (Hardware) Requires PKI	Encrypted text	Very Low	FOR OFFICIAL USE ONLY and information sensitive by aggregation where extra security is required due to compilation

Table 1. Security and Access Controls

3.2. Until such time as specific technical policy guidelines are formalized for all Internet services , Webmasters and users are encouraged to consult existing authoritative literature on security and access controls. Examples of such literature include, but are not limited to:

3.2.1. Carnegie Mellon University Software Engineering Institute, “Security for a Public Web Site,” CMU/SEI-SIM-002, August 1997.

3.2.2. National Institute of Standards and Technology (NIST), “Internet Security Policy: A Technical Guide,” http://csrc.nist.gov/isptg/html/ISPTG-Contents.html

3.2.3. Defense Information Systems Agency (DISA), “DISA/NCS World Wide Web (WWW) Handbook Version 2.2,” “http://www.disa.mil/handbook/toc.html"

4. TEXT OF PRIVACY AND SECURITY NOTICE

4.1. The following privacy and security notice may be tailored in the indicated areas by each organization sponsoring a publicly accessible Web site. The notice shall be approved by the appropriate local legal authority before use.

Link from Index.html pages -- "Please read this privacy and security notice."

( ) - indicates sections to be tailored at the installation level

[ ] - indicates hyperlinks

* - indicates information located at the hyperlink destination indicated

Quote:

PRIVACY AND SECURITY NOTICE

1. (DefenseLINK) is provided as a public service by the ([Office of the Assistant Secretary of Defense-Public Affairs] and the [Defense Technical Information Center]).

2. Information presented on (DefenseLINK) is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.

3. For site management, [information is collected]* for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

4. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with [National Archives and Records Administration Guidelines].

Agencies subject to DoD Directive 5240.1 shall add the following to paragraph 5: "All data collection activities are in strict accordance with DoD Directive 5240.1 (reference (p))."

6. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act.

7. If you have any questions or comments about the information presented here, please forward them to (us using the DefenseLINK [Comment Form]
_____ ***End Quote:***

* Link from above - "information is collected" to the following text:

NOTE: The information below should be tailored, if necessary, to show an accurate example of the specific information being collected.

Example: Information Collected from (DefenseLINK) for Statistical Purposes

Below is an example of the information collected based on a standard request for a World Wide Web document:

xxx.yyy.com - - [28/Jan/1997:00:00:01 -0500] "GET /DefenseLINK/news/nr012797.html HTTP/1.0" 200 16704 Mozilla 3.0/www.altavista.digital.com

xxx.yyy.com (or 123.123.23.12)-- this is the host name (or IP address) associated with the requester (you as the visitor). In this case, (...**.com**) the requester is coming from a commercial address. Depending on the requester's method of network connection, the host name (or IP address) may or may not identify a specific computer. Connections via many Internet Service Providers assign different IP addresses for each session, so the host name identifies only the ISP. The host name (or IP address) will identify a specific computer if that computer has a fixed IP address.

[28/Jan/1997:00:00:01 -0500] -- this is the date and time of the request

"GET /DefenseLINK/news/nr012797.html HTTP/1.0" -- this is the location of the requested file on (DefenseLINK)

200 -- this is the status code - 200 is OK - the request was filled

16704 -- this is the size of the requested file in bytes

Mozilla 3.0 -- this identifies the type of browser software used to access the page, which indicates what design parameters to use in constructing the pages

www.altavista.digital.com - this indicates the last site the person visited, which indicates how people find (DefenseLINK)

Requests for other types of documents use similar information. No other user-identifying information is collected.

4.2. The following notice and consent banner, approved by the DoD General Counsel p;-(reference (hh)), may be used on all DoD Web sites with security and access controls. This banner may be tailored by an organization but such modifications shall be accomplished in compliance with reference (hh), and shall be approved by the Component's General Counsel before use.

"This is a Department of Defense Computer System. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be

monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored.

Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes."